Newton Solney C of E Infant School e-Safety Policy

(Encompassing the

policies on Acceptable Use of the Internet and

E-safety)

Written by Heidi Elks in February 2014 and approved by Governors May 2014. To be reviewed annually or when there is an incident.

Reviewed by Governors: 18th May 2015
Reviewed by Governors: October 2018

Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to all staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors..

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents.

Safeguarding is a serious matter; at Newton Solney C of E Infant School we use technology and the Internet across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Newton Solney C of E Infant School website; upon review all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Students Acceptable Use Policy will be sent home with students at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Headteacher Name: Heidi Elks Signed:

Chair of Governors: Matt Tyler Signed:

Review Date: September 2018 Next Review: September 2019

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:

    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be also be the responsibility of the headteacher who is also the e-Safety Officer, with support from the senior teacher.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, governing body and parents.
- The designated e-Safety Officer has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

e-Safety Officer

The day-to-day duty of e-Safety Officer is devolved to the headteacher who is also the child protection officer and ICT co-ordinator.
The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the governors.
- Advise the staff and governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.

- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software,) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any e-safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer.
    - Passwords for staff will be a minimum of 8 characters.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any e-safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made), or in her absence to the senior teacher. If you are unsure the matter is to be raised with the Headteacher to make a decision.
- The reporting flowcharts contained within this e-safety policy are fully understood.

All Students

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

E-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents meetings, school newsletters the

school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

E-Safety Governor

Governor responsible for e-Safety is responsible for:

- to advise on changes to the e-safety policy.
- to establish the effectiveness (or not) of e-safety training and awareness in the school.
- to recommend further initiatives for e-safety training and awareness at the school.

Technology

Newton Solney C of E Infant School uses a range of devices including PC's, laptops, tablets and camera's. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use Capitabytes software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The headteacher is responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Governor and Capitabytes.

Email Filtering – we use Openhive software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message. It will also filter out emails with inappropriate language.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

Passwords – all staff will be unable to access any device without a unique staff username and password. Staff and student passwords will change if there has been a compromise. Camera's and tablets are not password protected.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task

is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as keydrives are to be scanned for viruses before use.

Safe Use of Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Photos and videos – Digital media such as photos and videos are covered in the schools' confidential pupil information form, and is re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

Social Networking – Is not allowed within school.
There is closed group of friends of Newton Solney C of E Infant on Facebook. Content is monitored by our senior teacher.
Staff must not name the school when using social networking sites at home and must not befriend parents or pupils. Staff must not post personal comments about the school.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school confidential pupil information form) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in his/her absence the senior teacher/Governor. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Newton Solney C of E Infant School will have an annual programme of training which is suitable to the audience.

e-Safety for students is embedded into the curriculum particularly within PSHE lessons; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the e-Safety Policy. Once you have read and understood both you must sign this policy sheet

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-safety officer and an incident sheet completed.

Social networking – is not allowed in school in accordance with the e-safety policy. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pendrive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the e-Safety Officer.

Viruses and other malware - any virus outbreaks are to be reported to the Headteacher as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

Copyright- you will respect copyright laws.

E-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with students.

NAME :

SIGNATURE : **DATE :**

Acceptable Use Policy – Students
Our Charter of Good Online Behaviour
Note: All Internet activity is subject to monitoring

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share personal information online about myself with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher/parents know if anybody asks me for personal information about myself on the Internet.

I will – let my teacher/parent know if anybody says or does anything to me that is hurtful or upsets me on the internet.

I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break these rules there will be consequences for my actions and my parents will be told.

Pupil's name……

My parents and I have read the Charter of Good Online Behaviour and I agree to follow it.

Signed (pupil) ……..

As parent or guardian, I have read, discussed and explained the Chart of Good Online Behaviour to my son/daughter. I understand that if he/she fails to follow this code, his/her individual access will be withdrawn and I will be informed.

Signed (parent) ……Date …….....